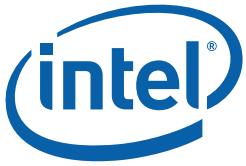


Intel® Core™ Duo Processor and Intel® Core™ Solo Processor on 65 nm Process

Specification Update

June 2006

Document Number: 309222-004

Contents

Revision History

Revision	Description	Date
-001	Initial release	January 2006
-002	• Updated Processor Identification (Table 1)	April 2006
-003	• Added Errata AE35-AE40 • Updated Errata A14 and AE29 • Updated Processor Identification (Table 1)	May 2006
-004	• Added Errata AE41-AE46 • Updated Processor Identification (Table 1) • Updated Description for Code ‘A’ in Summary Table of Changes	June 2006

§

Preface

This document is an update to the specifications contained in the documents listed in the following Affected Documents/Related Documents table. It is a compilation of device and document errata and specification clarifications and changes, and is intended for hardware system manufacturers and for software developers of applications, operating system, and tools.

Information types defined in the Nomenclature section of this document are consolidated into this update document and are no longer published in other documents. This document may also contain information that has not been previously published.

Affected Documents

Document Title	Document Number/Location
The Intel® Core™ Duo Processor and the Intel® Core™ Solo Processor on 65 nm Process Datasheet	309221-002

Related Documents

Document Title	Document Number/Location
IA-32 Intel® Architecture Software Developer's Manual, Volume 1: Basic Architecture	253665
IA-32 Intel® Architecture Software Developer's Manual, Volume 2A: Instruction Set Reference, A-M	253666
IA-32 Intel® Architecture Software Developer's Manual, Volume 2B: Instruction Set Reference, N-Z	253667
IA-32 Intel® Architecture Software Developer's Manual, Volume 3A: System Programming Guide	253668
IA-32 Intel® Architecture Software Developer's Manual, Volume 3B: System Programming Guide	253669
IA-32 Intel® Architecture Optimization Reference Manual	248966
Intel Processor Identification and the CPUID Instruction Application Note (AP-485)	241618

Nomenclature

S-Spec Number is a five-digit code used to identify products. Products are differentiated by their unique characteristics (e.g., core speed, L2 cache size, package type, etc.) as described in the processor identification information table. Care should be taken to read all notes associated with each S-Spec number

Errata are design defects or errors. Errata may cause the Intel® Core™ Duo processor and the Intel® Core™ Solo processor on 65 nm process behavior to deviate from published specifications. Hardware and software designed to be used with any given stepping must assume that all errata documented for that stepping are present on all devices.

Specification Changes are modifications to the current published specifications. These changes will be incorporated in the next release of the specifications.

Specification Clarifications describe a specification in greater detail or further highlight a specification's impact to a complex design situation. These clarifications will be incorporated in the next release of the specifications.

Documentation Changes include typos, errors, or omissions from the current published specifications. These changes will be incorporated in the next release of the specifications.

Note: Errata remain in the specification update throughout the product's lifecycle, or until a particular stepping is no longer commercially available. Under these circumstances, errata removed from the specification update are archived and available upon request. Specification changes, specification clarifications and documentation changes are removed from the specification update when the appropriate changes are made to the appropriate product specification or user documentation (datasheets, manuals, etc.).

§

Summary Tables of Changes

The following table indicates the Specification Changes, Errata, Specification Clarifications or Documentation Changes, which apply to the listed MCH steppings. Intel intends to fix some of the errata in a future stepping of the component, and to account for the other outstanding issues through documentation or Specification Changes as noted. This table uses the following notations:

Codes Used in Summary Table

Stepping

X:	Erratum, Specification Change or Clarification that applies to this stepping.
(No mark) or (Blank Box):	This erratum is fixed in listed stepping or specification change does not apply to listed stepping.

Status

Doc:	Document change or update that will be implemented.
PlanFix:	This erratum may be fixed in a future stepping of the product.
Fixed:	This erratum has been previously fixed.
NoFix:	There are no plans to fix this erratum.
Shaded:	This item is either new or modified from the previous version of the document.

Note: Each Specification Update item is prefixed with a capital letter to distinguish the product. The key below details the letters that are used in Intel's microprocessor Specification Updates:

A = Dual-Core Intel® Xeon® processor 7000 sequence
B = Mobile Intel® Pentium® II processor
C = Intel® Celeron® processor
D = Dual-Core Intel® Xeon™ Processor 2.80 GHz
E = Intel® Pentium® III processor
F = Intel® Pentium® processor Extreme Edition and Intel® Pentium® D processor
G = Intel® Pentium® III Xeon™ processor
H = Mobile Intel® Celeron® processor at 466 MHz, 433 MHz, 400 MHz, 366 MHz, 333 MHz, 300 MHz, and 266 MHz
J = 64-bit Intel® Xeon™ processor MP with 1-MB L2 cache
K = Mobile Intel® Pentium® III Processor - M
L = Intel® Celeron® D Processor
M = Mobile Intel® Celeron® processor
N = Intel® Pentium® 4 processor
O = Intel® Xeon™ processor MP
P = Intel® Xeon™ processor
Q = Mobile Intel® Pentium® 4 processor supporting Hyper-Threading Technology on 90-nm process technology
R = Intel® Pentium® 4 processor on 90 nm process
S = 64-bit Intel® Xeon™ processor with 800 MHz system bus
T = Mobile Intel® Pentium® 4 processor - M
V = Mobile Intel® Celeron® processor on 0.13 micron process in micro-FCPGA package
W = Intel® Celeron® M processor
X = Intel® Pentium® M processor on 90 nm process with 2-MB L2 cache
Y = Intel® Pentium® M processor
Z = Mobile Intel® Pentium® 4 processor with 533 MHz system bus
AA = Intel® Pentium® processor Extreme Edition and Intel® Pentium® D processor on 65 nm process
AB = Intel® Pentium® 4 processor on 65 nm process
AC = Intel® Celeron® processor in 478-Pin package
AE = Intel® Core™ Duo processor and Intel® Core™ Solo processor on 65 nm process

Number	C0	D0	Dual Core Only	Plans	ERRATA
AE1	X	X		No Fix	FST instruction with numeric and null segment exceptions may cause General Protection Faults to be missed and FP Linear Address (FLA) mismatch
AE2	X	X		No Fix	Code Segment limit violation may occur on 4-Gbyte limit check
AE3	X			No Fix	POPF and POPFD instructions that set the Trap Flag (TF) bit may cause unpredictable processor behavior
AE4	X	X		No Fix	REP MOVS operation in fast string mode continues in that mode when crossing into a page with a different memory type
AE5	X	X		No Fix	Memory Aliasing with inconsistent A and D bits may cause processor deadlock
AE6	X	X		No Fix	VM Bit Will Be Cleared on a Double Fault Handler
AE7	X	X		No Fix	Page with PAT (Page Attribute Table) Set to USWC (Uncacheable Speculative Write Combine) while associated MTRR (Memory Type Range Register) Is UC (Uncacheable) may consolidate to UC
AE8	X	X		No Fix	FXSAVE after FNINIT without an Intervening FP (floating point) instruction may save uninitialized values for FDP (x87 FPU Instruction Operand (Data) Pointer Offset) and FDS (x87 FPU Instruction Operand (Data) Pointer Selector)
AE9	X	X		No Fix	Under certain conditions LTR (Load Task Register) instruction may result in system hang
AE10	X	X		No Fix	Invalid entries in Page-Directory-Pointer-Table Register (PDPTR) may cause General Protection (#GP) exception if the reserved bits are set to one
AE11	X	X		No Fix	REP MOVS operation in fast string mode continues in that mode when crossing into a page with a different memory type
AE12	X	X		No Fix	FP inexact-result exception flag may not be set
AE13	X	X		No Fix	IFU/BSU deadlock may cause system hang
AE14	X	X		No Fix	MOV with debug register causes debug exception
AE15	X	X		No Fix	INIT does not clear global entries in the TLB
AE16	X	X		No Fix	Use of memory aliasing with inconsistent memory type may cause system hang
AE17	X	X		No Fix	Machine check exception may occur when interleaving code between different memory types
AE18	X			Plan Fix	Processor Digital Thermal Sensor (DTS) readout stops updating upon returning from C3/C4 State
AE19	X	X	X	No Fix	Data Prefetch Event Monitor (EMON) events can only be enabled on a single core

Number	C0	D0	Dual Core Only	Plans	ERRATA
AE20	X	X		No Fix	LOCK# asserted during a special cycle shutdown transaction may unexpectedly deassert
AE21	X	X		No Fix	Disable execution-disable bit (IA32_MISC_ENABLES [34]) is shared between cores
AE22	X	X		No Fix	Last Branch Records (LBR) updates may be incorrect after a task switch
AE23	X	X		No Fix	Address reported by Machine-Check Architecture (MCA) on single-bit L2 ECC errors may be incorrect
AE24	X	X		No Fix	Disabling of single-step On Branch Operation may be delayed following a POPFD instruction
AE25	X	X		No Fix	Performance monitoring counters that count external bus events may report incorrect values after processor power state transitions
AE26	X	X		No Fix	VERW/VERR/LSL/LAR instructions may unexpectedly update the Last Exception Record (LER) MSR
AE27	X	X		No Fix	General Protection (#GP) fault may not be signaled on data segment limit violation above 4-G limit
AE28	X	X		No Fix	Performance Monitoring Events for retired floating point operations (C1h) may not be accurate
AE29	X	X		No Fix	DR3 address match on MOVD/MOVQ/MOVNTQ memory store instruction may incorrectly increment performance monitoring count for saturating SIMD instructions executed (Event B1h)
AE30	X	X		No Fix	Global Pages in the Data Translation Look-Aside Buffer (DTLB) may not be flushed by RSM instruction before restoring the architectural state from SMRAM
AE31	X	X		No Fix	Data Breakpoint/Single Step on MOV SS/POP SS may be lost after entry into SMM
AE32	X	X		No Fix	CS limit violation on RSM may be serviced before higher priority Interrupts/Exceptions
AE33	X	X		No Fix	Hardware Prefetch Performance Monitoring Events may be counted inaccurately
AE34	X	X		No Fix	Pending x87 FPU Exceptions (#MF) following STI may be serviced before higher priority interrupts
AE35	X	X		No Fix	Programming the Digital Thermal Sensor (DTS) Threshold May Cause Unexpected Thermal Interrupts
AE36	X		X	Plan Fix	CPU_CLK_UNHALTED Performance Monitoring Event (3CH) Counts Clocks when the Processor is in the C1/C2 Processor Power States
AE37	X	X		No Fix	The Processor May Report a #TS Instead of a #GP Fault
AE38	X	X		No Fix	BTS Message May be Lost When the STPCLK# Signal is Active
AE39	X	X		No Fix	Certain Performance Monitoring Counters Related to Bus, L2 Cache and Power Management Are Inaccurate

Number	C0	D0	Dual Core Only	Plans	ERRATA
AE40	X	X		No Fix	A Write to an APIC Register Sometimes May Appear to Have Not Occurred
AE41	X	X	X	No Fix	IO_SMI Indication in SMRAM State Save Area May Be Set Incorrectly
AE42	X	X	X	No Fix	Simultaneous Access to the Same Page Table Entries by both Cores May Lead to Unexpected Processor Behavior
AE43	X		X	Plan Fix	IO_SMI Indication in SMRAM State Save Area May Be Lost
AE44	X	X	X	No Fix	Logical Processors May Not Detect Write-Back (WB) Memory Writes
AE45	X	X		No Fix	Last Exception Record (LER) MSRs May Be Incorrectly Updated
AE46	X	X		No Fix	SYSENTER/SYSEXIT Instructions Can Implicitly Load “Null Segment Selector” to SS and CS Registers

Number	SPECIFICATION CHANGES
	There are no Specification Changes in this Specification Update revision

Number	SPECIFICATION CLARIFICATIONS
	There are no Specification Clarifications in this Specification Update revision

Number	DOCUMENTATION CHANGES
	There are no Documentation Changes in this Specification Update revision

§

Identification Information

Component Identification via Programming Interface

The Intel® Core™ Duo processor and Intel® Core™ Solo processor on 65 nm process stepping can be identified by the following register contents:

Family[1]	Model[2]
0110	1110

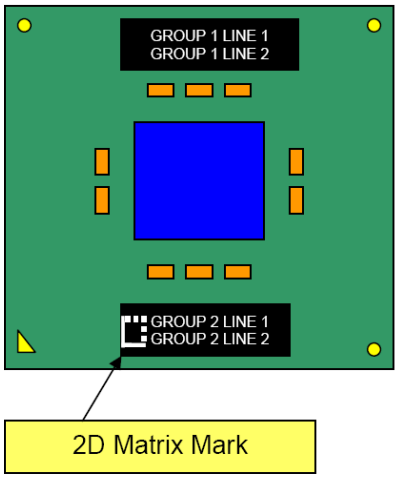
NOTES:

1. The family corresponds to bit [11:8] of the EDX register after RESET, bits [11:8] of the EAX register after the CPUID instruction is executed with a 1 in the EAX register, and the generation field of the Device ID register accessible through Boundary Scan.
2. The family corresponds to bit [7:4] of the EDX register after RESET, bits [7:4] of the EAX register after the CPUID instruction is executed with a 1 in the EAX register, and the generation field of the Device ID register accessible through Boundary Scan.

Cache and TLB descriptor parameters are provided in the EAX, EBX, ECX, and EDX registers after the CPUID instruction is executed with a 2 in the EAX register. Refer to the *Intel Processor Identification and the CPUID Instruction Application Note* (AP-485) for further information on the CPUID instruction.

Component Marking Information

Figure 1. Intel Core Duo Processor and Intel Core Solo Processor on 65 nm Process (Micro-FCPGA/FCBGA) S-Spec Markings



PRODUCTION MARK EXAMPLE:
GROUP 1 LINE 1: Unique Unit Identifier [Processor #]
GROUP 1 LINE 2: FPO S-SPEC#
GROUP 2 LINE 1: FREQUENCY/ L2 CACHE SIZE/ FSB
GROUP 2 LINE 1: INTEL m © '04

Table 1. Intel Core Duo Processor and Intel Core Solo Processor on 65 nm Process Identification Information

QDF/S-SPEC#	Processor #	Package	Stepping	CPUID	FSB(MHz)	Speed HFM/LFM (GHz)	Notes
SL9JP	T2700	Micro-FCPGA	D-0	06ECh	667	2.33/1.00	2
SL9K4	T2700	Micro-FCBGA	D-0	06ECh	667	2.33/1.00	2
SL99V	U2500	Micro-FCBGA	D-0	06ECh	533	1.20/.800	4
SL9JE	T2300E	Micro-FCPGA	D-0	06E8h	667	1.66/1.00	2
SL9JV	T2300E	Micro-FCBGA	D-0	06E8h	667	1.66/1.00	2
SL92X	T1400	Micro-FCBGA	C-0	06E8h	667	1.83/1.00	1,2
SL8W7	U1300	Micro-FCBGA	C-0	06E8h	533	1.06/0.80	4
SL8W6	U1400	Micro-FCBGA	C-0	06E8h	533	1.2/0.800	4
SL8VN	T2600	Micro-FCPGA	C-0	06E8h	667	2.16/1.00	2
SL8VP	T2500	Micro-FCPGA	C-0	06E8h	667	2.00/1.00	2
SL8VQ	T2400	Micro-FCPGA	C-0	06E8h	667	1.83/1.00	2
SL8VR	T2300	Micro-FCPGA	C-0	06E8h	667	1.66/1.00	2
SL8VS	T2600	Micro-FCBGA	C-0	06E8h	667	2.16/1.00	2
SL8VT	T2500	Micro-FCBGA	C-0	06E8h	667	2.00/1.00	2
SL8VU	T2400	Micro-FCBGA	C-0	06E8h	667	1.83/1.00	2
SL8VV	T2300	Micro-FCBGA	C-0	06E8h	667	1.66/1.00	2
SL92U	T1500	Micro-FCPGA	C-0	06E8h	667	2.00/1.00	1,2
SL92V	T1400	Micro-FCPGA	C-0	06E8h	667	1.83/1.00	1,2
SL8VY	T1300	Micro-FCPGA	C-0	06E8h	667	1.66/1.00	1,2
SL92W	T1500	Micro-FCBGA	C-0	06E8h	667	2.00/1.00	1,2
SL92X	T1400	Micro-FCBGA	C-0	06E8h	667	1.83/1.00	1,2
SL8W3	T1300	Micro-FCBGA	C-0	06E8h	667	1.66/1.00	1,2
SL8VW	L2400	Micro-FCBGA	C-0	06E8h	667	1.66/1.00	3
SL8VX	L2300	Micro-FCBGA	C-0	06E8h	667	1.50/1.00	3

NOTES:

1. Single Core Processor
2. VCC_CORE=1.300-1.1625/1.000-0.7625 V for HFM/LFM Range; Deeper Sleep OVID Range=0.850-0.550 V; Deep C4 OVID Range=0.800-0.500 V.
3. VCC_CORE=1.2125-1.000/1.000-0.7625 V for HFM/LFM Range; Deeper Sleep OVID Range=0.850-0.550 V; Deep C4 OVID Range=0.800-0.500 V.
4. VCC_CORE=1.0500-0.950/0.9375 V for HFM range /LFM Range; Deeper Sleep OVID Range=0.800-0.750 V; Deep C4 OVID Range=0.750-0.650 V.

§

Errata

AE1. FST Instruction with Numeric and Null Segment Exceptions May Cause General Protection Faults to Be Missed and FP Linear Address (FLA) Mismatch

Problem: FST instruction combined with numeric and null segment exceptions may cause General Protection Faults to be missed and FP Linear Address (FLA) mismatch.

Implication: This is a rare condition that may result in a system hang. Intel has not observed this erratum with any commercially available software, or system.

Workaround: None.

Status: For the steppings affected, see the Summary Tables of Changes.

AE2. Code Segment Limit Violation May Occur on 4-Gbyte Limit Check

Problem: Code Segment limit violation may occur on 4-Gbyte limit check when the code stream wraps around in a way that one instruction ends at the last byte of the segment and the next instruction begins at 0x0.

Implication: This is a rare condition that may result in a system hang. Intel has not observed this erratum with any commercially available software, or system.

Workaround: Avoid code that wraps around segment limit.

Status: For the steppings affected, see the Summary Tables of Changes.

AE3. POPF and POPFD Instructions That Set the Trap Flag (TF) Bit May Cause Unpredictable Processor Behavior

Problem: In some rare cases, POPF and POPFD instructions that set the Trap Flag (TF) bit in the EFLAGS register (causing the processor to enter Single-Step mode) may cause unpredictable processor behavior.

Implication: Single-Step operation is typically enabled during software debug activities, not during normal system operation.

Workaround: There is no workaround for Single-Step operation in commercially available software. For debug activities on custom software the POPF and POPFD instructions could be immediately followed by a NOP instruction to facilitate correct execution.

Status: For the steppings affected, see the Summary Tables of Changes.

AE4. REP MOVS Operation in Fast String Mode Continues in That Mode When Crossing into a Page with a Different Memory Type

Problem: A fast “REP MOVS” operation continues to be handled in fast mode when the string operation crosses a page boundary into an Uncacheable (UC) memory type. Also if the fast string operation crosses a page boundary into a WC memory region, the processor does not self snoop the WC memory region. This may result in incorrect data for the WC portion of the operation if those cache lines were previously cached as WB (through aliasing) and modified.

Implication: String elements should be handled by the processor at the native operand size in UC memory. In the event that the WB to WC aliasing case occurs, the end result could vary— from benign software execution to operating system or application failure. Intel has not observed either aspects of this erratum in commercially available software.

Workaround: Software operating within Intel’s recommendation will not require WB and WC memory aliased to the same physical address.

Status: For the steppings affected, see the Summary Tables of Changes.

AE5. Memory Aliasing with Inconsistent A and D Bits May Cause Processor Deadlock

Problem: In the event that software implements memory aliasing by having two Page Directory Entries (PDEs) point to a common Page Table Entry (PTE) and the Accessed and Dirty bits for the two PDEs are allowed to become inconsistent the processor may become deadlocked.

Implication: This erratum has not been observed with commercially available software.

Workaround: Software that needs to implement memory aliasing in this way should manage the consistency of the Accessed and Dirty bits.

Status: For the steppings affected, see the Summary Tables of Changes.

AE6. VM Bit Will Be Cleared on a Double Fault Handler

Problem: Following a task switch to a Double Fault Handler that was initiated while the processor was in virtual-8086 (VM86) mode, the VM bit will be incorrectly cleared in EFLAGS.

Implication: When the OS recovers from the double fault handler, the processor will no longer be in VM86 mode.

Workaround: None.

Status: For the steppings affected, see the Summary Tables of Changes.

AE7. Page with PAT (Page Attribute Table) Set to USWC (Uncacheable Speculative Write Combine) While Associated MTRR (Memory Type Range Register) Is UC (Uncacheable) May Consolidate to UC

Problem: A page whose PAT memory type is USWC while the relevant MTRR memory type is UC, the consolidated memory type may be treated as UC (rather than WC, as specified in *IA-32 Intel® Architecture Software Developer's Manual*).

Implication: When this erratum occurs, the memory page may be as UC (rather than WC). This may have a negative performance impact.

Workaround: None identified.

Status: For the steppings affected, see the Summary Tables of Changes.

AE8. FXSAVE after FNINIT without an Intervening FP (Floating Point) Instruction May Save Uninitialized Values for FDP (x87 FPU Instruction Operand (Data) Pointer Offset) and FDS (x87 FPU Instruction Operand (Data) Pointer Selector)

Problem: An FXSAVE after FNINIT without an intervening FP instruction may save uninitialized values for FDP and FDS.

Implication: When this erratum occurs, the values for FDP/FDS in the FXSAVE structure may appear to be random values. These values will be initialized by the first FP instruction executed after the FXRSTOR that restore the saved floating point state. Any FP instruction with memory operand will initialize FDP/FDS. Intel has not observed this erratum with any commercially available software.

Workaround: After an FINIT, do not expect the FXSAVE memory image to be correct, until at least one FP instruction with a memory operand has been executed.

Status: For the steppings affected, see the Summary Tables of Changes.

AE9. Under Certain Conditions, LTR (Load Task Register) Instruction May Result in System Hang

Problem: An LTR instruction may result in a system hang if all the following conditions are met:

1. Invalid data selector of the TR (Task Register) resulting with either #GP (General Protection Fault) or #NP (Segment Not Present Fault).
2. GDT (Global Descriptor Table) is not 8-bytes aligned.
3. Data BP (breakpoint) is set on cache line containing the descriptor data. When this erratum occurs, the memory page may be as UC (rather than WC). This may have a negative performance impact.

Implication: This erratum may result in system hang if all conditions have been met. This erratum has not been observed in commercial operating systems or software. For performance reasons, GDT is typically aligned to 8-bytes.

Workaround: Software should align GDT to 8-bytes.

Status: For the steppings affected, see the Summary Tables of Changes.

AE10. Invalid Entries in Page-Directory-Pointer-Table Register (PDPTR) May Cause General Protection (#GP) Exception If the Reserved Bits Are Set to One

Problem: Invalid entries in the Page-Directory-Pointer-Table Register (PDPTR) that have the reserved bits set to one may cause a General Protection (#GP) exception.

Implication: Intel has not observed this erratum with any commercially available software.

Workaround: Do not set the reserved bits to one when PDPTR entries are invalid.

Status: For the steppings affected, see the Summary Tables of Changes.

AE11. REP MOVS Operation in Fast String Mode Continues in That Mode When Crossing into a Page with a Different Memory Type

Problem: A fast “REP MOVS” operation continues to be handled in fast mode when the string operation crosses a page boundary into an Uncacheable (UC) memory type. Also if the fast string operation crosses a page boundary into a WC memory region, the processor does not self snoop the WC memory region. This may result in incorrect data for the WC portion of the operation if those cache lines were previously cached as WB (through aliasing) and modified.

Implication: String elements should be handled by the processor at the native operand size in UC memory. In the event that the WB to WC aliasing case occurs, the end result could vary— from benign software execution to operating system or application failure. Intel has not observed either aspects of this erratum in commercially available software.

Workaround: Software operating within Intel’s recommendation will not require WB and WC memory aliased to the same physical address.

Status: For the steppings affected, see the Summary Tables of Changes.

AE12. FP Inexact-Result Exception Flag May Not Be Set

Problem: When the result of a floating-point operation is not exactly representable in the destination format (1/3 in binary form, for example), an inexact-result (precision) exception occurs. When this occurs, the PE bit (bit 5 of the FPU status word) is normally set by the processor. Under certain rare conditions, this bit may not be set when this rounding occurs. However, other actions taken by the processor (invoking the software exception handler if the exception is unmasked) are not affected. This erratum can only occur if the floating-point operation which causes the precision exception is immediately followed by one of the following instructions:

- FST m32real
- FST m64real
- FSTP m32real
- FSTP m64real
- FSTP m80real
- FIST m16int
- FIST m32int
- FISTP m16int
- FISTP m32int
- FISTP m64int

Note that even if this combination of instructions is encountered, there is also a dependency on the internal pipelining and execution state of both instructions in the processor.

Implication: Inexact-result exceptions are commonly masked or ignored by applications, as it happens frequently, and produces a rounded result acceptable to most applications. The PE bit of the FPU status word may not always be set upon receiving an inexact-result exception. Thus, if these exceptions are unmasked, a floating-point error exception handler may not recognize that a precision exception occurred. Note that this is a “sticky” bit, i.e., once set by an inexact-result condition, it remains set until cleared by software.

Workaround: This condition can be avoided by inserting two NOP instructions between the two floating-point instructions.

Status: For the steppings affected, see the Summary Tables of Changes.

AE13. IFU/BSU Deadlock May Cause System Hang

Problem: A lockable instruction with memory operand that spans across two pages may, given some rare internal conditions, hang the system.

Implication: When this erratum occurs, the system may hang. Intel has not observed this erratum with any commercially available software or system.

Workaround: Lockable data should always be contained in a single page.

Status: For the steppings affected, see the Summary Tables of Changes.

AE14. MOV with Debug Register Causes Debug Exception

Problem: When in V86 mode, if a MOV instruction is executed on debug registers, a general-protection exception (#GP) should be generated. However, in the case when the general detect enable flag (GD) bit is set, the observed behavior is that a debug exception (#DB) is generated instead.

Implication: With debug-register protection enabled (i.e., the GD bit set), when attempting to execute a MOV on debug registers in V86 mode, a debug exception will be generated instead of the expected general-protection fault.

Workaround: In general, operating systems do not set the GD bit when they are in V86 mode. The GD bit is generally set and used by debuggers. The debug exception handler should check that the exception did not occur in V86 mode before continuing. If the exception did occur in V86 mode, the exception may be directed to the general-protection exception handler.

Status: For the steppings affected, see the Summary Tables of Changes.

AE15. INIT Does Not Clear Global Entries in the TLB

Problem: INIT may not flush a TLB entry when:

1. The processor is in protected mode with paging enabled and the page global enable flag is set (PGE bit of CR4 register)
2. G bit for the page table entry is set
3. TLB entry is present in TLB when INIT occurs.

Implication: Software may encounter unexpected page fault or incorrect address translation due to a TLB entry erroneously left in TLB after INIT.

Workaround: Write to CR3, CR4 or CR0 registers before writing to memory early in BIOS code to clear all the global entries from TLB.

Status: For the steppings affected, see the Summary Tables of Changes.

AE16. Use of Memory Aliasing with Inconsistent Memory Type May Cause System Hang

Problem: Software that implements memory aliasing by having more than one linear addresses mapped to the same physical page with different cache types may cause the system to hang. This would occur if one of the addresses is non-cacheable used in code segment and the other a cacheable address. If the cacheable address finds its way in instruction cache, and non-cacheable address is fetched in IFU, the processor may invalidate the non-cacheable address from the fetch unit. Any micro-architectural event that causes instruction restart will expect this instruction to still be in fetch unit and lack of it will cause system hang.

Implication: This erratum has not been observed with commercially available software.

Workaround: Although it is possible to have a single physical page mapped by two different linear addresses with different memory types, Intel has strongly discouraged this practice as it may lead to undefined results. Software that needs to implement memory aliasing should manage the memory type consistency.

Status: For the steppings affected, see the Summary Tables of Changes.

AE17. Machine Check Exception May Occur When Interleaving Code between Different Memory Types

Problem: A small window of opportunity exists where code fetches interleaved between different memory types may cause a machine check exception. A complex set of micro-architectural boundary conditions is required to expose this window.

Implication: Interleaved instruction fetches between different memory types may result in a machine check exception. The system may hang if machine check exceptions are disabled. Intel has not observed the occurrence of this erratum while running commercially available applications or operating systems.

Workaround: Software can avoid this erratum by placing a serializing instruction between code fetches between different memory types.

Status: For the steppings affected, see the Summary Tables of Changes.

AE18. Processor Digital Thermal Sensor (DTS) Readout Stops Updating upon Returning from C3/C4 state

Problem: Digital Thermal Sensor (DTS) Readout is provided in IA32_THERM_STATUS bits 22:16. Upon waking up from C3/C4 low-power state, the DTS readout will no longer be updated.

Implication: Upon waking up from C3/C4 low-power state, software cannot rely on DTS readout any thermal threshold interrupts that are enabled in IA32_THERM_INTERRUPT, will also be affected.

Workaround: It is possible for BIOS to contain a workaround for this erratum.

Status: For the steppings affected, see the Summary Tables of Changes.

AE19. Data Prefetch Event Monitor (EMON) Events Can Only Be Enabled on a Single Core

Problem: Current implementation of Data Prefetch EMON events allow counting only for a single core at a time.

Implication: Dual-core support for counting Data Prefetch EMON events is not currently available.

Workaround: Software should enable Data Prefetch EMON events on one core at a time.

Status: For the steppings affected, see the Summary Tables of Changes.

AE20. LOCK# Asserted during a Special Cycle Shutdown Transaction May Unexpectedly Deassert

Problem: During a processor shutdown transaction, when LOCK# is asserted and if a DEFER# is received during a snoop phase and the Locked transaction is pipelined on the front side bus (FSB), LOCK# may unexpectedly deassert.

Implication: When this erratum occurs, the system may hang during shutdown. Intel has not observed this erratum with any commercially available systems or software.

Workaround: .None identified.

Status: For the steppings affected, see the Summary Tables of Changes.

AE21. Disable Execution-Disable Bit (IA32_MISC_ENABLES [34]) Is Shared between Cores

Problem: The bit 34 of the IA32_MISC_ENABLES Model Specific Register (MSR) is shared between the execution cores.

Implication: Both cores will operate according to the shared value of bit IA32_MISC_ENABLES [34].

Workaround: None identified.

Status: For the steppings affected, see the Summary Tables of Changes.

AE22. Last Branch Records (LBR) Updates May Be Incorrect after a Task Switch

Problem: A Task-State Segment (TSS) task switch may incorrectly set the LBR_FROM value to the LBR_TO value.

Implication: The LBR_FROM will have the incorrect address of the Branch Instruction.

Workaround: None identified.

Status: For the steppings affected, see the Summary Tables of Changes.

AE23. Address Reported by Machine-Check Architecture (MCA) on Single-Bit L2 ECC Errors May Be Incorrect

Problem: When correctable single-bit ECC errors occur in the L2 cache the address is logged in the MCA address register (MCi_ADDR). Under some scenarios, the address reported may be incorrect.

Implication: Software should not rely on the value reported in MCi_ADDR, for Single-bit L2 ECC errors

Workaround: None identified.

Status: For the steppings affected, see the Summary Tables of Changes.

AE24. Disabling of Single-Step On Branch Operation May Be Delayed following a POPFD Instruction

Problem: Disabling of Single-step On Branch Operation may be delayed, if the following conditions are met:

1. “Single Step On Branch Mode” is enabled (DebugCtlMSR.BTF and EFLAGS.TF are set)
2. POPFD used to clear EFLAGS.TF
3. A jump instruction (JMP, Jcc, etc.) is executed immediately after POPFD

Implication: Single-step On Branch mode may remain in effect for one instruction after the POPFD instruction disables it by clearing the EFLAGS.TF bit.

Workaround: There is no workaround for Single-Step operation in commercially available software. The workaround for custom software is to execute at least one instruction following POPFD before issuing a JMP instruction.

Status: For the steppings affected, see the Summary Tables of Changes.

AE25. Performance Monitoring Counters That Count External Bus Events May Report Incorrect Values after Processor Power State Transitions

Problem: Performance monitoring counters that count external bus events operate when the processor is in the Active state (C0). If a processor transitions to a new power state, these Performance monitoring counters will stop counting, even if the event being counted remains active.

Implication: After transitioning between processor power states, software may observe incorrect counts in Performance monitoring counters that count external bus events.

Workaround: None identified.

Status: For the steppings affected, see the Summary Tables of Changes.

AE26. VERW/VERR/LSL/LAR Instructions May Unexpectedly Update the Last Exception Record (LER) MSR

Problem: The LER MSR may be unexpectedly updated, if the resultant value of the Zero Flag (ZF) is zero after executing the following instructions:

1. VERR (ZF=0 indicates unsuccessful segment read verification)
2. VERW (ZF=0 indicates unsuccessful segment write verification)
3. LAR (ZF=0 indicates unsuccessful access rights load)
4. LSL (ZF=0 indicates unsuccessful segment limit load)

Implication: The value of the LER MSR may be inaccurate if VERW/VERR/LSL/LAR instructions are executed after the occurrence of an exception.

Workaround: Software exception handlers that rely on the LER MSR value should read the LER MSR before executing VERW/VERR/LSL/LAR instructions.

Status: For the steppings affected, see the Summary Tables of Changes.

AE27. General Protection (#GP) Fault May Not Be Signaled on Data Segment Limit Violation above 4-G Limit

Problem: Memory accesses to flat data segments (base = 00000000h) that occur above the 4-G limit (0ffffffffh) may not signal a #GP fault.

Implication: When such memory accesses occur, the system may not issue a #GP fault.

Workaround: Software should ensure that memory accesses do not occur above the 4-G limit (0ffffffffh).

Status: For the steppings affected, see the Summary Tables of Changes.

AE28. Performance Monitoring Events for Retired Floating Point Operations (C1h) May Not Be Accurate

Problem: Performance Monitoring Events that count retired floating point operations may be too high.

Implication: The Performance Monitoring Event may have an inaccurate count.

Workaround: None identified.

Status: For the steppings affected, see the Summary Tables of Changes.

AE29. DR3 Address Match on MOVD/MOVQ/MOVNTQ Memory Store Instruction May Incorrectly Increment Performance Monitoring Count for Saturating SIMD Instructions Executed (Event B1h)

Problem: Performance monitoring for Event CFH normally increments on saturating SIMD instruction retired. Regardless of DR7 programming, if the linear address of a retiring memory store MOVD/MOVQ/MOVNTQ instruction executed matches the address in DR3, the CFH counter may be incorrectly incremented.

Implication: The value observed for performance monitoring count for saturating SIMD instructions retired may be too high. The size of error is dependent on the number of occurrences of the conditions described above, while the counter is active.

Workaround: None identified.

Status: For the steppings affected, see the Summary Tables of Changes.

AE30. Global Pages in the Data Translation Look-Aside Buffer (DTLB) May Not Be Flushed by RSM Instruction before Restoring the Architectural State from SMRAM

Problem: Resume from System Management Mode (RSM) does not flush global pages from DTLB before the System Management RAM (SMRAM) loads.

Implication: If SMM turns on paging with global paging enabled and then maps any of linear addresses of SMRAM using global pages, RSM load may load data from the wrong location.

Workaround: Do not use global pages in system management mode.

Status: For the steppings affected, see the Summary Tables of Changes.

AE31. Data Breakpoint/Single Step on MOV SS/POP SS May Be Lost after Entry into SMM

Problem: Data Breakpoint/Single Step exceptions are normally blocked for one instruction following MOV SS/POP SS instructions. Immediately after executing these instructions, if the processor enters SMM (System Management Mode), upon RSM (resume from SMM) operation, normal processing of Data Breakpoint/Single Step exceptions is restored.

Because of this erratum, Data Breakpoints/Single step exceptions on MOVSS/POPSS instructions may be lost under one of the following conditions.

1. Following SMM entry and after RSM, the next instruction to be executed is HLT or MWAIT
2. SMM entry after executing MOV SS/POP SS is the result of executing an I/O instruction that triggers a synchronous SMI (System Management Interrupt).

Implication: Data Breakpoints/Single step operation on MOV SS/POP SS instructions may be unreliable in the presence of SMIs.

Workaround: None Identified.

Status: For the steppings affected, see the Summary Tables of Changes.

AE32. CS Limit Violation on RSM May Be Serviced before Higher Priority Interrupts/Exceptions

Problem: When the processor encounters a CS (Code Segment) limit violation, a #GP (General Protection Exception) fault is generated after all higher priority Interrupts and Exceptions are serviced. Because of this erratum, if RSM (Resume from System Management Mode) returns to execution flow where a CS limit violation occurs, the #GP fault may be serviced before a higher priority Interrupt or Exception (e.g., NMI (Non-Maskable Interrupt), Debug break(#DB), Machine Check (#MC), etc.).

Implication: Operating systems may observe a #GP fault being serviced before higher priority Interrupts and Exceptions.

Workaround: None Identified.

Status: For the steppings affected, see the Summary Tables of Changes.

AE33. Hardware Prefetch Performance Monitoring Events May Be Counted Inaccurately

Problem: Hardware prefetch activity is not accurately reflected in the Hardware Prefetch Performance Monitoring.

Implication: This erratum may cause inaccurate counting for all Hardware Prefetch Performance Monitoring Events.

Workaround: None identified.

Status: For the steppings affected, see the Summary Tables of Changes.

AE34. Pending x87 FPU Exceptions (#MF) following STI May Be Serviced before Higher Priority Interrupts

Problem: Interrupts that are pending prior to the execution of the STI (Set Interrupt Flag) instruction are serviced immediately after the STI instruction is executed. Because of this erratum, if following STI, an instruction that triggers a #MF is executed while STPCLK#, Enhanced Intel SpeedStep® Technology transitions or Intel® Thermal Monitor 1 events occur, the pending #MF may be serviced before higher priority interrupts.

Implication: Software may observe #MF being serviced before higher priority interrupts.

Workaround: None identified.

Status: For the steppings affected, see the Summary Tables of Changes.

AE35. Programming the Digital Thermal Sensor (DTS) Threshold May Cause Unexpected Thermal Interrupts

Problem: Software can enable DTS thermal interrupts by programming the thermal threshold and setting the respective thermal interrupt enable bit. When programming DTS value, the previous DTS threshold may be crossed. This will generate an unexpected thermal interrupt.

Implication: Software may observe an unexpected thermal interrupt occur after reprogramming the thermal threshold.

Workaround: In the ACPI/OS implement a workaround by temporarily disabling the DTS threshold interrupt before updating the DTS threshold value.

Status: For the steppings affected, see the Summary Tables of Changes.

AE36. CPU_CLK_UNHALTED Performance Monitoring Event (3CH) Counts Clocks When the Processor Is in the C1/C2 Processor Power States

Problem: The CPU_CLK_UNHALTED performance monitoring event should only count clocks when the processor is running. However, due to this erratum, CPU_CLK_UNHALTED performance monitoring event may count clocks when the cores have been halted in the C1/C2 processor power states. The count may be incorrect when the two cores are not in C1/C2 state simultaneously

Implication: The CPU_CLK_UNHALTED performance monitoring event may read a somewhat larger value than expected.

Workaround: None identified.

Status: For the steppings affected, see the Summary Tables of Changes.

AE37. The Processor May Report a #TS Instead of a #GP Fault

Problem: A jump to a busy TSS (Task-State Segment) may cause a #TS (invalid TSS exception) instead of a #GP fault (general protection exception).

Implication: Operation systems that access a busy TSS may get invalid TSS fault instead of a #GP fault. Intel has not observed this erratum with any commercially available software.

Workaround: None identified.

Status: For the steppings affected, see the Summary Tables of Changes.

AE38. BTS Message May Be Lost When the STPCLK# Signal Is Active

Problem: STPCLK# is asserted to enable the processor to enter a low-power state (C2, C3, etc.). Under some circumstances, when STPCLK# becomes active, a pending BTS (Branch Trace Store) message may be either lost and not written or written with corrupted branch address to the Debug Store area.

Implication: BTS messages may be lost in the presence of STPCLK# assertions.

Workaround: None identified.

Status: For the steppings affected, see the Summary Tables of Changes.

AE39. Certain Performance Monitoring Counters Related to Bus, L2 Cache and Power Management Are Inaccurate

Problem: All Performance Monitoring Counters in the ranges 21H-3DH and 60H-7FH may have inaccurate results up to +/- 7.

Implication: There may be a small error in the affected counts.

Workaround: None identified.

Status: For the steppings affected, see the Summary Tables of Changes.

AE40. A Write to an APIC Register Sometimes May Appear to Have Not Occurred

Problem: With respect to the retirement of instructions, stores to the uncacheable memory-based APIC register space are handled in a non-synchronized way. For example if an instruction that masks the interrupt flag, e.g., CLI, is executed soon after an uncacheable write to the Task Priority Register (TPR) that lowers the APIC priority, the interrupt masking operation may take effect before the actual priority has been lowered. This may cause interrupts whose priority is lower than the initial TPR, but higher than the final TPR, to not be serviced until the interrupt enabled flag is finally set, i.e., by STI instruction. Interrupts will remain pending and are not lost.

Implication: In this example the processor may allow interrupts to be accepted but may delay their service.

Workaround: This non-synchronization can be avoided by issuing an APIC register read after the APIC register write. This will force the store to the APIC register before any subsequent instructions are executed. No commercial operating system is known to be impacted by this erratum.

Status: For the steppings affected, see the Summary Tables of Changes.

AE41. IO_SMI Indication in SMRAM State Save Area May Be Set Incorrectly

Problem: The IO_SMI bit in SMRAM's location 7FA4H is set to "1" by the CPU to indicate a System Management Interrupt (SMI) occurred as the result of executing an instruction that reads from an I/O port. Due to this erratum, the IO_SMI bit may be incorrectly set by:

- A non-I/O instruction.
- SMI is pending while a lower priority event interrupts
- A REP I/O read
- An I/O read that redirects to MWAIT.

Implication: .SMM handlers may get false IO_SMI indication.

Workaround: The SMM handler has to evaluate the saved context to determine if the SMI was triggered by an instruction that read from an I/O port. The SMM handler must not restart an I/O instruction if the platform has not been configured to generate a synchronous SMI for the recorded I/O port address.

Status: For the steppings affected, see the Summary Tables of Changes.

AE42. Simultaneous Access to the Same Page Translation Entries by Both Cores May Lead to Unexpected Processor Behavior

Problem: When the following conditions occur simultaneously, this may create a rare internal condition which may lead to unexpected processor behavior.

- One core is updating a page table entry, including the processor setting the Accessed and/or Dirty bits in the PTE as the result of an access
- The other core is using the same translation entry.

Implication: Unpredictable behavior in the processor may lead to livelock and shutdown. Intel has not observed this erratum with any commercially available software.

Workaround: None Identified.

Status: For the steppings affected, see the Summary Tables of Changes.

AE43. IO_SMI Indication in SMRAM State Save Area May Be Lost

Problem: The IO_SMI bit in SMRAM's location 7FA4H is set to "1" by the CPU to indicate a System Management Interrupt (SMI) that occurred as the result of executing an instruction that read from an I/O port. Due to this erratum, the setting of the IO_SMI bit may be lost. This may happen if following the instruction that read from an I/O port, there is an instruction with a memory operand that results in one of the following:

- Update of a Page Table Entry (PTE) Accessed (A) or Dirty (D) bits.
- Page Fault (#PF)
- A REP I/O read
- Unaligned Memory access where either address of the first or last byte of the access (ex: (Address1stByte AND NOT 0x3F) OR (AddressLastByte AND NOT 0x3F)) is equal to the address in one of the Debug Address Registers (DR0-DR3) (e.g., DRx AND NOT 0x3F) as long as any address breakpoint is enabled through the Debug Control Register (DR7).

Implication: SMI handlers may not be able to identify the occurrence of I/O SMIs.

Workaround: It is possible for BIOS to contain a workaround for this erratum.

Status: For the steppings affected, see the Summary Tables of Changes.

AE44. Logical Processors May Not Detect Write-Back (WB) Memory Writes

Problem: Multiprocessor systems may use polling of memory semaphores to synchronize software activity. Because of this erratum, if a logical processor is polling a WB memory location while it is being updated by another logical processor, the update may not be detected.

Implication: System may livelock due to polling loop and undetected semaphore change. Intel has not observed this erratum on commercially available systems.

Workaround: It is possible for BIOS to contain a workaround for this erratum.

Status: For the steppings affected, see the Summary Tables of Changes.

AE45. Last Exception Record (LER) MSRs May be Incorrectly Updated

Problem: The LASTINTTOIP and LASTINTFROMIP MSRs (1DDH-1DEH) may contain incorrect values after the following events: masked SSE2 floating-point exception, StopClk, NMI and INT.

Implication: The value of the LER MSR may be incorrectly updated to point to a SIMD Floating-Point instruction even though no exception occurred on that instruction or to point to an instruction that was preceded by a StopClk interrupt or rarely not to be updated on Interrupts (NMI and INT).

Workaround: None identified.

Status: For the steppings affected, see the Summary Tables of Changes.

AE46. SYSENTER/SYSEXIT Instructions Can Implicitly Load "Null Segment Selector" to SS and CS Registers

Problem: According to the processor specification, attempting to load a null segment selector into the CS and SS segment registers should generate a General Protection Fault (#GP). Although loading a null segment selector to the other segment registers is allowed, the processor will generate an exception when the segment register holding a null selector is used to access memory. However, the SYSENTER instruction can implicitly load a null value to the SS segment selector. This can occur if the value in SYSENTER_CS_MSR is between FFF8h and FFFBh when the SYSENTER instruction is executed. This behavior is part of the SYSENTER/SYSEXIT instruction definition; the content of the SYSTEM_CS_MSR is always incremented by 8 before it is loaded into the SS. This operation will set the null bit in the segment selector if a null result is generated, but it does not generate a #GP on the SYSENTER instruction itself. An exception will be generated as expected when the SS register is used to access memory, however. The SYSEXIT instruction will also exhibit this behavior for both CS and SS when executed with the value in SYSENTER_CS_MSR between FFF0h and FFF3h, or between FFE8h and FFEBh, inclusive.

Implication: These instructions are intended for operating system use. If this erratum occurs (and the OS does not ensure that the processor never has a null segment selector in the SS or CS segment registers), the processor's behavior may become unpredictable, possibly resulting in system failure.

Workaround: Do not initialize the SYSTEM_CS_MSR with the values between FFF8h and FFFBh, FFF0h and FFF3h, or FFE8h and FFEBh before executing SYSENTER or SYSEXIT.

Status: For the steppings affected, see the Summary Tables of Changes.

§

Specification Changes

There are no specification changes in this specification update revision.

Note: All specification changes will be incorporated into a future version of the *Intel® Core™ Duo Processor and Intel® Core™ Solo Processor on 65 nm Process Datasheet*.

§

Specification Clarifications

There are no specification clarifications in this specification update revision.

Note: All specification changes will be incorporated into a future version of the *Intel® Core™ Duo Processor and Intel® Core™ Solo Processor on 65 nm Process Datasheet.*

§

Documentation Changes

There are no documentation changes in this specification update revision.

Note: All specification changes will be incorporated into a future version of the appropriate Intel® Core™ Duo Processor and Intel® Core™ Solo Processor on 65 nm Process Datasheet.

Note: Documentation changes for *IA-32 Intel® Architecture Software Developer's Manuals volumes 1, 2A, 2B, 3A and 3B* will be posted in a separate document *IA-32 Intel® Architecture and Intel® Extended Memory 64 Technology Software Developer's Manual Documentation Changes*. Follow the link below to become familiar with this file.

http://developer.intel.com/design/pentium4/specupdt/252046.htm§